The CLOUD Act

A new way for international tribunals to access digital evidence

Völkerrechtsblog 2019-04-08T10:00:18

From violent protests in Sudan to airstrikes in Syria, access to online open source material and digital information is becoming essential for the fight against impunity. Open Source Information is publicly available information that anyone can lawfully obtain by request, purchase, or observation. Today's international criminal and human rights investigations increasingly rely on digital data, such as content posted on social media platforms, to support criminal proceedings and ultimately hold the perpetrators of atrocities accountable. However, take-downs by companies like *Facebook*, *Youtube* and *Twitter* make it harder for prosecutors and other law enforcement bodies to access essential material needed for their investigations. The recently enacted Clarifying Lawful Overseas Use of Data Act ("Cloud Act") in the United States ("U.S.") may be a legislative response to this need.

This blog post provides a brief answer to two questions, using the International Criminal Court ("ICC") as a case study: (i) whether the term "foreign government," as used in the Cloud Act, reasonably includes international organizations or tribunals, which would enable them to enter into an executive agreement with the U.S. for information sharing purposes, and if not, (ii) whether the Cloud Act permits a foreign government that has an executive agreement with the U.S. to acquire and share information obtained with international tribunals such as the ICC for investigation and prosecution purposes.

The *Microsoft* Case: Where it all started

In 2018, the pending Supreme Court case *United States v. Microsoft* pressured Congress to enact the Cloud Act as a legislative response to the ambiguity generated by the increased use of digital technologies globally and the correlated need for law enforcement to access digital data. The *Microsoft* case centered on whether a U.S. law enforcement agency that had served Microsoft with a search warrant for emails in a drug trafficking investigation could get access. The emails' content was stored at a Microsoft Data Center in Dublin, Ireland. Microsoft refused to give up the information, arguing that a U.S. judge has no authority to issue a warrant for information stored abroad. Before the Supreme Court could render a judgment, Congress passed the Cloud Act, and clarified the reach of US courts regarding the matter of data extraterritoriality.

Today, the Cloud Act expands the power of the U.S. government to require service providers to release data to U.S. law enforcement that is in their possession or control, whether or not the data is located inside the U.S. Additionally, the Cloud Act authorizes the U.S. government to enter into executive agreements with foreign

governments for the purpose of information sharing. These agreements aim to streamline the complex process that foreign nations have to go through to seek data from U.S.-based providers, who hold most of the world's electronic communications.

Importantly, these executive agreements are limited to requests from "foreign governments" related to cases involving "serious" crimes that do not target U.S. persons. This raises the question of whether international tribunals can be considered "foreign governments" and enter into executive agreements with the U.S. to access digital data. If not, does the Cloud Act offer other avenues that enable international tribunals to access digital information?

What is a "foreign government"?

The Cloud Act does not define the term "foreign government." Section 2713 (1) (A) states only that a foreign government is one "(i) with which the [U.S.] has an executive agreement that has entered into force under section 2523" and "(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities […]." Thus, there is no explicit definition of what *type* of entity is considered a foreign government.

Despite this, the Cloud Act's plain language suggests that the term "foreign government" only applies to States and not to international institutions. For instance, various sections require that the *domestic laws* of the foreign government satisfy specific requirements in order for the U.S. to enter into an executive agreement. However, an international tribunal does not have "domestic law" *per se*. The ICC, for instance, is enabled by and subject to the Rome Statute and the Rules of Procedures and Evidence but not domestic legislation.

Title 18 of the United States Code ("USC"), of which the Cloud Act is part, provides more definitional guidance, however. Chapter 1, Section 11 defines the term foreign government as "any government, faction, or body of insurgents within a country with which the United States is at peace, irrespective of recognition by the United States."

This definition arguably applies to all of Title 18 pursuant to the "standard principle of statutory construction … that identical words and phrases within the same statute should normally be given the same meaning." This statutory interpretation finds further support in the non-interchangeable use of "foreign government" and "international organizations" in other sections of Title 18. For example, 18 USC § 970, which governs protection of property occupied by foreign governments, uses the terms "foreign government" and "international organizations" separately. Thus, the term "foreign government" should not be read to include international organizations or tribunals such as the ICC. Because of this, the U.S. and the ICC are unlikely to be able to enter into an executive agreement for purposes of the Cloud Act.

Sharing information with the ICC through another qualified foreign government

Another way for the ICC to access the data held by U.S. providers could be *through* a qualifying "foreign government." In theory, a foreign government that has an executive agreement with the United States could request information and pass that information on to the ICC.

Both the plain language and the intent underlying the Cloud Act suggest this is possible. With regards to intent, the Act is supposed to make access to digital information easier to access for the purpose of prosecuting serious crimes. Interpreting the Cloud Act as allowing States to cooperate with the ICC would comply with the Act's goal of assisting the prosecution of serious crimes. Per section 2523 (b) (3) (D) (ii), foreign governments may issue requests "for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crimes." Similarly, as stated in article 1 of the Rome Statue, the ICC "shall have the power to exercise its jurisdiction over persons for the most serious crimes of international concern," indicating an alignment of mandate. Moreover, Article 54 (3) of the Rome Statute enables the Prosecutor to "enter in agreements and seek cooperation from States and intergovernmental organizations," and State Parties are bound to assist the ICC in its investigations. Therefore, this common objective, combined with States' obligation to collaborate with the court, strongly suggest that a foreign government may (and perhaps even should) pass information to the ICC to facilitate the prosecution of serious crimes.

This interpretation is also supported by the Act's plain language. A third-party state that qualifies as a "qualifying foreign government" and respects various human rights standards set forth in section 2523 (b) B) ii), could request information about a suspect from another State through an executive agreement. The standards that states must respect include civil and political rights such as prohibitions on arbitrary arrest and detention, fair trial rights, freedom of expression, etc.

Additionally, the Cloud Act does not prohibit a "foreign government" from requesting information about a citizen from a certain country and pass that information to the ICC, as the Cloud Act only prohibits the exchange of information with third-party *governments*. More specifically, section 2523 (3) (c) prohibits a foreign government that has an executive agreement with the U.S. from requesting or obtaining information about a person for the purpose of passing it to the U.S. government or to a third party-government. Thus, a State can ask for information about a citizen under investigation from a country X and pass the information to an international organization, such as a tribunal, that is not included in the definition of "foreign government" or "third-party government." For example, per the Cloud Act, Canada may enter into an executive agreement with the United States and then require information about an alleged war criminal from Uganda, and then share that information with the ICC.

The only limit to this type of collaboration is the explicit prohibition in the Cloud Act from targeting U.S. persons. Section 2523 (3) (A) provides that a "foreign government may not intentionally target a [U.S.] person or a person located in the [U.S.]," and Section 2523 (3) (B) of the Cloud Act specifies that a "foreign government may not target a non-[U.S.] person located outside the [U.S.] if the purpose is to obtain information concerning a United States person or a person

located in the [U.S.].” This prohibition, however, implicitly allows States to request information about citizens or residents from other countries than the U.S.

Therefore, nothing in the Cloud Act appears to prevent a qualified foreign government that has entered into an executive agreement with the U.S. from sharing information about a person from a country outside with the ICC or other international tribunal.

Conclusion

In sum, in the Cloud Act, the term “foreign government” does not include international organizations such as the ICC. Thus, such organizations cannot enter into executive agreements with the U.S. for Cloud Act purpose. However, a third-party state that meets the requisite conditions can acquire information about a non-U.S. person and transfer that information to an international organization such as the ICC. This blog post uses the case study of the ICC notably because the Rome Statute specifically requires states’ assistance for prosecuting alleged criminals. It follows, however, that this may apply to other independent international tribunals, who prosecute individuals for international crimes, such as a future potential tribunal for Syria. However, at the moment, only the ICC falls under this category. These executive agreements between States could also lead to information sharing with their national war crime units that are part of the same governmental entity and who prosecute individuals for international crimes. This interpretation of the Cloud Act could be one of the solutions to the ongoing fragmentation and disruption between national privacy laws, by facilitating the operability of transnational data for US companies who hold most of the world’s data on their servers with States who have robust human rights law protection. This framework, in which State cooperation with international organizations for prosecution purposes will, in the end, facilitate access to digital information to advance the prosecution of international criminals—combatting impunity and fostering justice.

Mélina Cardinal-Bradette holds a LL.B. from Université Laval in Quebec, Canada and is a LL.M. candidate at UC Berkeley School of Law with a specialization in international law. She is also a member of the Human Rights Center Technology and Human Rights Program’s Investigations Lab legal team (2018-2019).

Fabian Unser-Nad is a LL.M. candidate at UC Berkeley School of Law with a specialization in international law. He is the Legal Team Manager of the Human Rights Center Technology and Human Rights Program’s Investigations Lab (2018-2019).

Cite as: Mélina Cardinal-Bradette & Fabian Unser-Nad, “The CLOUD Act: A new way for international tribunals to access digital evidence”, *Völkerrechtsblog*, 8 April 2019.